United States Department of Agriculture

Office of the Chief *Information Officer*

1400 Independence Avenue SW

Washington, DC 20250

APR 12 2010

TO: Agency Chief Information Officers
Departmental Management
Information System Security Program Managers

FROM: Charles McClam
Deputy Chief Information Officer
Office of the Chief Information Officer

SUBJECT: Logging and Handling of Data Extracts of Sensitive Information and Personally Identifiable Information

The United States Department of Agriculture (USDA) takes its responsibility to appropriately handle Sensitive Information (SI), and Personally Identifiable Information (PII) seriously. SI/PII data is subject to loss, compromise, or unauthorized disclosure if not handled properly, especially when that data is removed or extracted from its originating environment.

In accordance with Office of Management and Budget (OMB) guidance contained in M-07-16, the Department is responsible for implementing policy to ensure that data extracts containing SI/PII are erased when they are no longer needed. For purposes of this memorandum, a data extract is defined as multiple records of information that are downloaded or copied from an USDA database system and maintained in electronic format outside of the originating system. This memorandum is limited to data extracts that contain SI/PII data.

This memorandum provides Department-wide guidance for logging all computer-readable data extracts from databases holding SI/PII data.

Additionally, it is limited to data extracts that are physically removed from USDA premises via electronic transmission, laptop, file, CD, diskette, memory key, or any other portable storage device. This includes data extracts downloaded via USDA's virtual private network (VPN) to any external device. Using the VPN to access files and data (without download to an external device) is NOT subject to this policy.

The risks to extracted SI/PII data can be reduced in several ways:

- If the sensitive data is not needed in the extract, do not include it.
- Limit the number of records in the extract to the smallest number needed.
- Delete the extract as soon as it is no longer needed.

Agencies must follow the audit logging guidance in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems".

The audit log should contain sufficient information, at a minimum:

- Establish what type of event occurred;
- When (date and time) the event occurred;
- Where the event occurred;
- The source of the event;
- The outcome (success or failure) of the event; and
- The identity of any user/subject associated with the event.

For more detailed information, refer to http://csrc.nist.gov/publications/PubsSPs.html.

Encrypting SI/PII Data Extracts

USDA employees, contractors, and partners are also reminded that any data extract that is placed on removable media devices, such as CD-ROMs, removable hard drives, and thumb drives must be encrypted using the Federal Information Processing Standard (FIPS) 197, *Advanced Encryption Standard (AES)* http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. Sensitive data extracts are not permitted to be moved to non-government assets.

Handling and Transporting of SI/PII Data Extracts

USDA employees, contractors, and partners are reminded that they are required to follow existing USDA policies on the handling and transporting of SI/PII Data. When physical transport of data is necessary, portable media containing PII or other sensitive data must be encrypted *first,* then transported by the United States Postal Service or another authorized delivery service (e.g. United Parcel Service, Federal Express, DHL, or private courier). Portable media should be double-wrapped in an opaque package or container that is sealed sufficiently to prevent inadvertent opening and to show signs of tampering. The decryption key must be transmitted via a separate package or alternate channel. The package must be sent via a certified carrier with an ability to track pickup, receipt, transfer, and delivery. When necessary, portable media may be transmitted by interoffice mail provided it is double-wrapped to afford sufficient protection against inadvertent or unauthorized access.

In addition to the information contained herein; USDA employees, contractors, and partners are reminded that they must also comply with USDA policy on Sensitive But Unclassified (SBU) Information Protection, which can be found at http://www.ocio.usda.gov/directives/doc/DM3550-002.pdf.

Additional questions and answers regarding data extracts of sensitive information can be found at http://csrc.nist.gov/drivers/documents/OMB/OMB-M-07-16-Data-Extract-FAQ.pdf. Agencies are encouraged to perform re-occurring ad hoc reviews to ensure adherence to this guidance. If you have any questions regarding this memorandum, please contact Ms. Ray Payton, Chief Privacy Officer at (202) 720-8755 or ravoyne.payton@ocio.usda.gov.